Cyber Threat to Critical Infrastructure 2010-2015

Increased Control System Exposure

Peter D. Gasper
Idaho National Laboratory

24 Sep 2008
208 526 4597
Peter.gasper@inl.gov

Idaho National Laboratory

Cyber Threat to Critical Infrastructure 2010-2015

Overview

- INL role in Critical Infrastructure Protection (CIP)
- Threat assessment at INL
- Trends in Critical Infrastructure (CI) Control Systems (CS)
- Implications of technology transfer
- Increasing interest in CS Vulnerabilities
- Russo-Georgian Conflict – Did it change the environment?

INL Role in CIP

Protecting the Systems Controlling Our Infrastructure

- ***Control Systems Capabilities***
  - Supervisory Control and Data Acquisition (SCADA)/CS Vulnerability Testing
  - Asset owner Vulnerability Assessments
  - Analysis of vulnerabilities
  - Training
    - SANS SCADA Summit
    - Red Team/Blue Team training

- ***Primary Facilities & Resources***
  - Critical Infrastructure Test Range
    - **SCADA Test Bed**
    - **Power Grid Test Bed**
    - Mock Chemical Mixing Facility
    - Wireless Test Bed
- ***Full Scale testing with real infrastructure***

Idaho National Laboratory

Access/Working Relationships With Global Vendors

Objectives

- Create secure CS environments that improve the security posture of our nation's critical infrastructure.

Capabilities

- Fully functional SCADA systems and Energy Management Systems (EMS)
- Fully functional Distributed Control Systems (DCS)
- Safety systems and protective components
- Real world configurations and consequence testing
- Ability to generate CS data traffic
- Vendor and asset owner partnerships through DOE/ DHS programs
  - Large SCADA/EMS systems
  - On-site assessments

Threat Assessment at INL

Threat = Capability + Intent + Opportunity

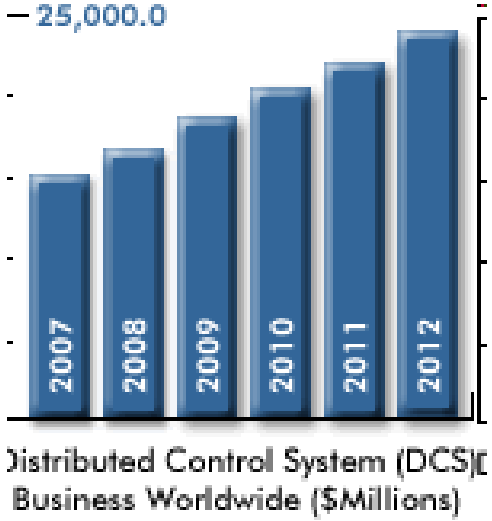
- ***Vulnerability assessment is a primary role at INL***
  - Threat Assessment is secondary and is more difficult, but --
    - Vulnerability research can point to threat Capability; and
    - It can also describe various types of Opportunity
- ***A Threat assumes existence of a Threat Actor***
  - Threat actors are variously defined
  - US-CERT lists: National governments, terrorists, industrial spies, organized crime groups, hacktivists, hackers
- ***INL is pursuing means to:***
  - Characterize threat actors; and
  - Estimate their potential Capability

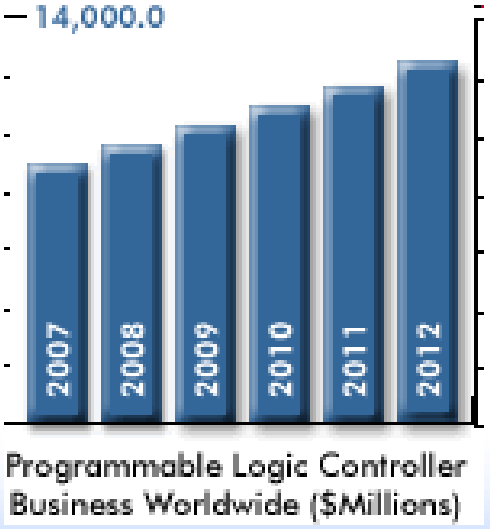
Critical Infrastructure CS Trends

- ***Current trends indicate:***
  - Greatly expanded CS presence, and
  - Increased unprotected CS exposure
- ***Major trends into 2010-2015 include:***
  - Proliferation of control systems,
  - Increased digital and IP base,
  - Expanded use of wireless communications, and
  - Lagging security measure implementation

Trend 1 – Proliferation of Control Systems

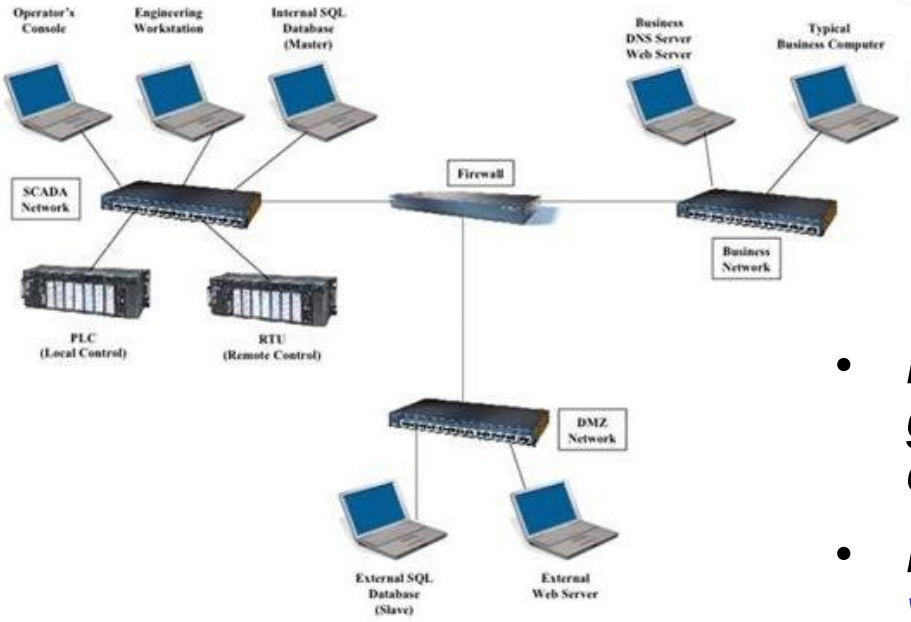
- ***The World SCADA market expected to grow at an 8.9% compounded annual rate into 2012***
- ***Nearly all CI sectors moving to advanced CS***
- ***CI CS will have greatly increased and more complex presence in 2010-2015***





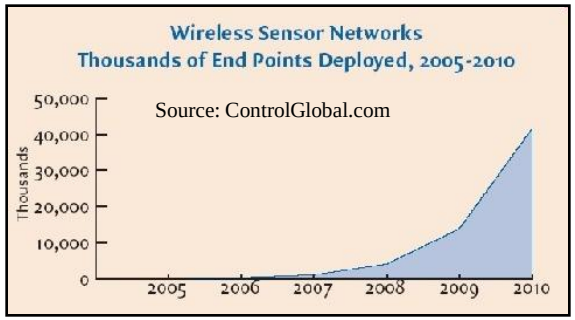
Source: www.arcweb.com

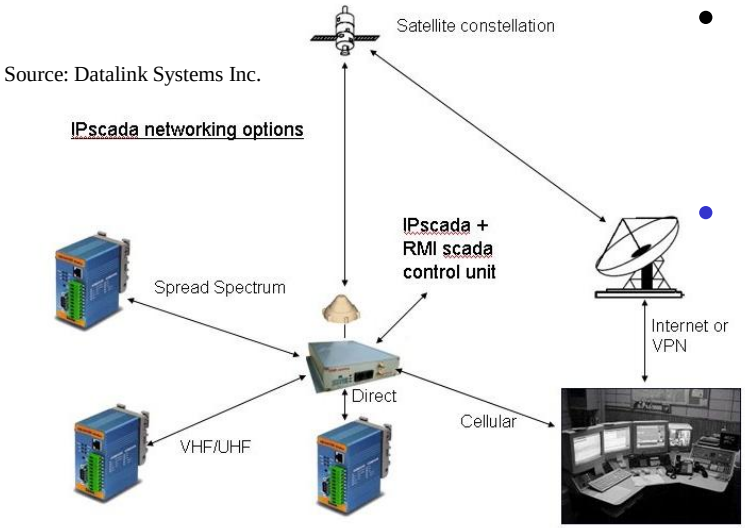
Trend 2 – Increased Digital and IP Base



- ***Several different protocols in use***
  - Causes confusion among users,
  - The most popular are:
    - International Electrotechnical Commission (IEC) 60870-5 series, specifically IEC 60870-5-101
    - Distributed Network Protocol version 3 (DNP3).
- ***Number of protocols continue to grow <u>despite</u> standardization efforts***
- ***Proliferation of protocols adds to vulnerability concerns***

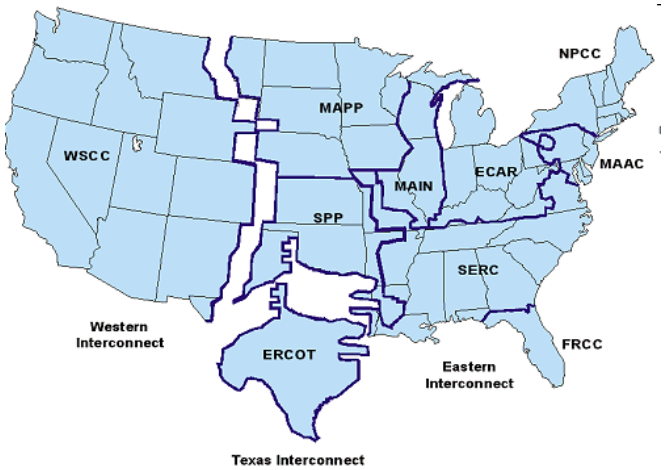
Trend 3 - Expanded Wireless Comms





- ***Wireless CS expected to grow at <u>31.8%</u> compound annual rate into 2012***
- ***Radio frequency access points increase potential for malicious entry***
- ***Exposure for CI CS will greatly increase in 2010-2015***

Trend 4 –Security Measure Impediments



- ***Successful vulnerability detection programs … <u>but</u>***
- ***Implementation of security measures lags behind***
  - Multiple private & governmental agencies/jurisdictions are involved
  - Natural delays occur in bringing software & hardware solutions into the market
  - Vulnerability mitigation is costly

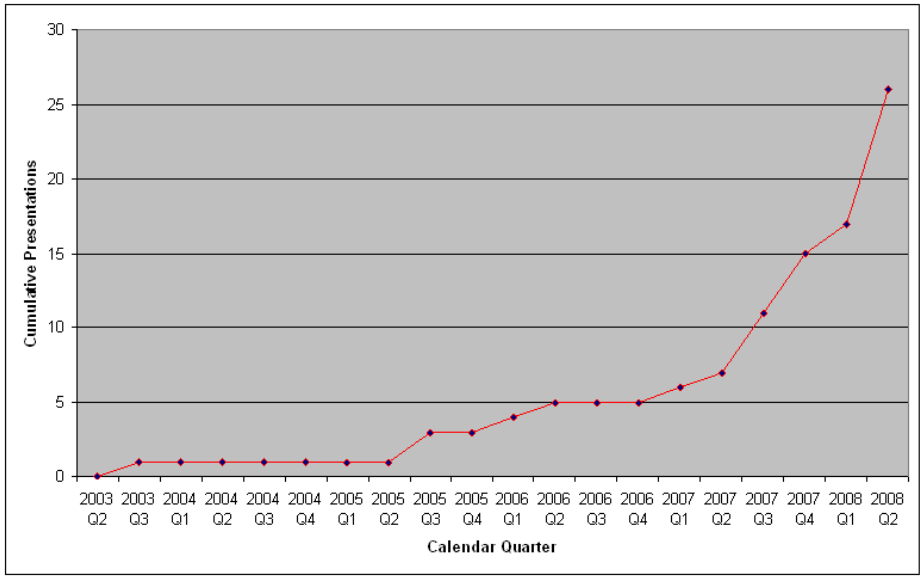
Impediments prolong unprotected exposure of CI CS

Implications of Technology Transfer

- ***CI CS proliferation is a global phenomenon***
- ***CI CS presence & exposure is cluttering the operational environment***
- ***No longer an exclusive Western domain***
- ***CS technology proliferation allows threat actors to perform "independent" vulnerability research***

Increasing Interest in CS Vulnerabilities

- ***DEFCON-15 signaled heightened interest in CS vulnerabilities***
- ***CI CS vulnerabilities now discussed worldwide***

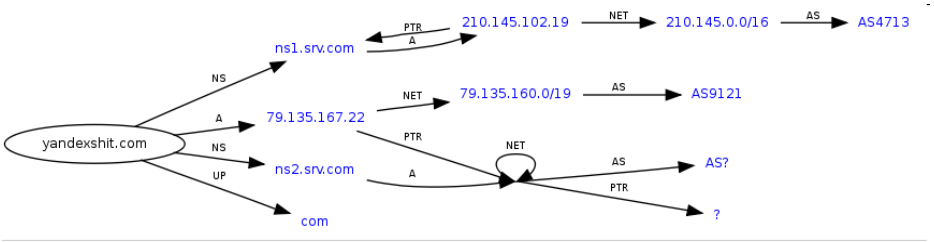


位于德克萨斯州奥斯汀地区3Com公司旗下TippingPoint公司的安全调研员Ganesh Devarajan于日前出席DefCon黑客研讨会时发表了上述观点。

未来黑客利用的这些软件漏洞通常隐匿于大型电脑上的“数据采集与监视控制”（SCADA：supervisory control and data acquisition）系统，这些电脑被广泛的应用在石油和天然气管道，水处理以及电力传输线路上，甚至用于大型工厂的工艺控制。 Source: www.cnxhacker.com

Russo-Georgian Conflict

Did it change the environment?



- ***Beyond the media hype***
  - Malicious cyber activity, primarily DDoS attacks, preceded & coincided with military activity;
  - “Neutral” servers were captured and “impressed” into combat as “botnets”; and
  - Real-time forensics were stymied
- ***Implications***
  - These tactics will be refined and blended;
  - No country’s flag of cyber neutrality will be respected;
  - U.S. CI CS servers will be at risk during “any” conflict; and
  - Forensics will be time-late in supporting CI protection

Conclusion

The Operational Environment – 2010-2015

- ***CI CS worldwide will:***
  - Display greater presence
  - Be subject to increased unprotected exposure
- ***Threat actors will have access to:***
  - More technical anti-CS Capability
  - Expanded Opportunity
- ***National defense and CI protection will be hampered by:***
  - Time-late indications & warning
  - Degraded identification of threat actors
  - U.S. CI CS servers used as “cyber sanctuaries”

Threat =

Capability
+
Intent
+
Opportunity